



# ACCESSING INFORMATION ON INTERNET: TOOLS AND TECHNIQUES TO BYPASS FILTRATION

Dr. Nand Kumar Singh

Assistant Professor, Computer Science & Application, Loyola College Kunkuri, Jashpur, SGGVV University Ambikapur, Chhattisgarh, India

## ABSTRACT

Internet filtration is the control or suppression of what can be accessed, published, or viewed on the Internet. Filtering can be based on relatively static blacklist or be determined more dynamically based on real-time examination of the information being exchanged.

There are many individuals, corporations and governments who favor Internet filtration. Internet filtration takes many forms. For example, governments may block regular e-mail services in order to compel citizens to use government e-mail that can be easily monitored, filtered, or shut down. Parents can control the content their minor children access. A university may prevent students from accessing Facebook from the library. An Internet café owner can block peer-to-peer file sharing. Authoritarian governments may censor reports on human rights abuses.

People have widely varying views about the legitimacy or illegitimacy of these forms. Just as many individuals, corporations and governments see the Internet as a source of dangerous information that must be controlled; there are many individuals and groups who are working hard to ensure that the Internet, and the information on it, is freely available to everyone who wants it. There is a vast amount of energy, from commercial, non-profit and volunteer groups, devoted to creating tools and techniques to bypass Internet censorship, resulting in a number of methods to bypass Internet filters.

**KEYWORDS:** Internet filtration, Bypass Internet censorship, Government

## 1. INTRODUCTION

### 1.1 Internet

The Internet developed from the ARPANET, which was funded by the US government to support projects within the government and at universities and research laboratories in the US – but grew over time to include most of the world's large universities and the research arms of many technology companies<sup>[1][2][3]</sup>.

Several countries have adopted laws requiring the state to work to ensure that Internet access is broadly available and/or preventing the state from unreasonably restricting an individual's access to information and the Internet.

### 1.2 Internet Filtration

As early as the 1990's when proliferation of the Internet started, countries were already enacting legislation on Internet censorship<sup>[4]</sup>. Internet censorship increased since 1997 and was marked by disparities in policy, types of governance, divergent approaches in adherence to international human rights' treaties, restrictions on Internet access and content affected<sup>[4]</sup>. Gradually Internet censorship has become more visible, gaining attention from scholars and research institutions in different disciplines including media and communication, information technology, law, political science, and economics.

## 2. LITRATURE REVIEW

The Internet can act as a social, cultural, commercial, educational, and entertainment global communication system whose legitimate purpose is to benefit and empower people and lower barriers in access to information. It is the largest global, decentralized communication network with invisible boundaries<sup>[5]</sup>, and owned by nobody<sup>[4]</sup>. It can enhance the exercising of human rights and fundamental freedoms, such as the right to freedom of expression, access to information, right to communication, and the right to assembly<sup>[5]</sup>. Any person can be empowered<sup>[6]</sup>, communicate instantly with a huge international audience<sup>[4]</sup>, or publish<sup>[7]</sup>. It is especially important in the academic world<sup>[8]</sup> and in schools<sup>[9]</sup>. While governments recognize that the benefits of the Internet far outweigh its negative aspects, they maintain that the negative aspects cannot be ignored<sup>[4]</sup>.

### 2.1 Arguments for and against Internet Filtration

Supporters of censorship argue that information over the Internet is controlled because it carries a certain amount of potentially harmful or illegal content that can instigate criminal activities and terrorism. However, those that are against the issue indicate that the primary motivation for censorship is often political<sup>[10]</sup> and they are concerned about the impact on intellectual freedom<sup>[11]</sup>.

The rationale for Internet censorship differs from country to

country. Cohen(1997) identified reasons common to many countries:

- National security (information on weapons' making, illegal drugs and protection from terrorism);
- Protection of minors (information on abuse, forms of marketing, violence and pornography);
- Protection of human dignity (incitement to racial hatred or discrimination);
- Economic security (fraud, pirating of credit cards);
- Information security (malicious hacking);
- Protection of privacy (protection against unauthorized communication of personalized data, electronic harassment, spamming);
- Protection of reputation (defamation, unlawful comparative advertising);
- Protection of intellectual property (the unauthorized distribution of works under copyright such as music, software, books, etc).

## 2.2 Internet Filtration in specific countries

Warf (2011) classifies countries' censorship as:

- **Worst Internet censors** e.g. China, Burma/Myanmar, Vietnam and Iran.
- **Severe Internet censors** e.g. Russia, Belarus, Pakistan, Arab World countries such as Saudi Arabia, Jordan, Bahrain, etc.
- **Moderate Internet censors** e.g. Thailand, Malaysia, Singapore, Indonesia, India, Central Asia, United Arab Emirates, Sub Saharan Africa and Latin America.
- **Light Internet censors** e.g. Latin America countries, Southern and Eastern Europe.
- **Uncensored Internet** e.g. Western Europe and USA. (For the latter it might be that there are forms of implied censorship not noted.)

Deibert *et al.* (2008; 2010; 2012) outline a summary of selected countries based on the OpenNet Initiative research. They explain that legal and regulatory frameworks, including Internet law, the state of Internet access and infrastructure, the level of economic development, and the quality of governance institutions, are central to determining which countries resort to filtering and how they choose to implement Internet content controls. They distinguish the following categories of filtering:

- **Political:** the focus is on websites that express views opposing governments. In most cases the content is related to human rights, freedom of expression, minority rights and religious movements.
- **Social:** the focus is on content related to sexuality, gambling, illegal drugs and alcohol and other issues considered illicit.
- **Conflict/security:** focuses on content related to armed conflicts, border disputes, and militant groups.
- **Internet tools:** websites that provide email, Internet hosting, search, translation, voice-over Internet Protocol, and telephone service, as well as circumvention methods.

### 2.2.1 Ten Most Censored Countries

The 2015 list of 10 Most Censored Countries according to CPJ's annual publication

1. Eritrea
2. North Korea
3. Saudi Arabia
4. Ethiopia
5. Azerbaijan
6. Vietnam
7. Iran
8. China
9. Myanmar
10. Cuba

## 2.3 Internet Filtration in India

Internet censorship in India is selectively practiced by both federal and state governments. While there is no sustained government policy or strategy to block access to Internet content on a large scale, measures for removing content have become more common in recent years. However, websites blocked either by the government or Internet service providers can often be accessed through proxy servers.

In June 2000, the Indian Parliament created the Information Technology (IT) Act to provide a legal framework to regulate Internet use and commerce, including digital signatures, security, and hacking [12]. The act criminalizes the publishing of obscene information electronically and grants police powers to search any premises without a warrant and arrest individuals in violation of the act. A 2008 amendment to the IT Act reinforced the government's power to block Internet sites and content and criminalized sending messages deemed inflammatory or offensive [13].

In 2003, the Government of India established the Indian Computer Emergency Response Team (CERTIN) to ensure Internet security [14]. Its stated mission is "to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration" [15]. CERTIN is the agency that accepts and reviews requests to block access to specific websites. All licensed Indian ISPs must comply with CERTIN decisions. There is no review or appeals process. Many institutions, including the Ministry of Home Affairs, courts, the intelligence services, the police and the National Human Rights Commission, may call on it for specialist expertise. By stretching the prohibition against publishing obscene content to include the filtering of Web sites, CERTIN was empowered to review complaints and act as the sole authority for issuing blocking instructions to the Department of Telecommunications (DOT). Many have argued that giving CERTIN this power through executive order violates constitutional jurisprudence holding that specific legislation must be passed before the government can encroach on individual rights [12].

### 2.3.1 OpenNet Initiative report

The Open Net Initiative classified India as engaged in "selective" Internet filtering in the political, conflict/security, social, and Internet tools areas in 2011 [12][16]. ONI describes India as:

- A stable democracy with a strong tradition of press freedom that nevertheless continues its regime of Internet filtering.

However, India's selective censorship of blogs and other content, often under the guise of security, have also been met with significant opposition.

- Indian ISPs continue to selectively filter Web sites identified by authorities. However, government attempts at filtering have not been entirely effective because blocked content has quickly migrated to other Web sites and users have found ways to circumvent filtering. The government has also been criticized for a poor understanding of the technical feasibility of censorship and for haphazardly choosing which Web sites to block.

### 2.3.2 Reporters Without Borders report

In March 2012, Reporters Without Borders added India to its list of "countries under surveillance", [17] stating that:

- Since the Mumbai bombings of 2008, the Indian authorities have stepped up Internet surveillance and pressure on technical service providers, while publicly rejecting accusations of censorship. The national security policy of the world's biggest democracy is undermining freedom of expression and the protection of Internet users' personal data.

### 2.3.3 Freedom House report

Freedom House's *Freedom on the Net 2014* report gives India a Freedom on the Net Status of "Partly Free" with a rating of 42 (scale from 0 to 100, lower is better). Its Obstacles to Access was rated 13 (0-25scale), Limits on Content was rated 10 (0-35scale) and Violations of User Rights was rated 19 (0-40scale) [18].

The *Freedom on the Net 2012* report, says:[19]

- India's overall Internet Freedom Status is "Partly Free", unchanged from 2009.
- India has a score of 39 on a scale from 0 (most free) to 100 (least free), which places India among 20 out of the 47 countries worldwide that were included in the 2012 report. India ranked 14 out of 37 countries in the 2011 report.
- India ranks third out of the eleven countries in Asia included in the 2012 report.
- Prior to 2008, censorship of Internet content by the Indian government was relatively rare and sporadic.
- Following the November 2008 terrorist attacks in Mumbai, which killed 171 people, the Indian Parliament passed amendments to the Information Technology Act (ITA) that expanded the government's censorship and monitoring capabilities.
- While there is no sustained government policy or strategy to block access to Internet content on a large scale, measures for removing certain content from the web, sometimes for fear they could incite violence, have become more common.
- Pressure on private companies to remove information that is perceived to endanger public order or national security has increased since late 2009, with the implementation of the amended ITA. Companies are required to have designated employees to receive government blocking requests, and assigns up to seven years' imprisonment private service providers—including ISPs, search engines,

and cybercafés—that do not comply with the government's blocking requests.

- Internet users have sporadically faced prosecution for online postings, and private companies hosting the content are obliged by law to hand over user information to the authorities.
- In 2009, the Supreme Court ruled that bloggers and moderators can face libel suits and even criminal prosecution for comments posted on their websites.
- Prior judicial approval for communications interception is not required and both central and state governments have the power to issue directives on interception, monitoring, and decryption. All licensed ISPs are obliged by law to sign an agreement that allows Indian government authorities to access user data.

### 2.4 Different forms of Internet Filtration

Emerging tools and techniques for Internet censorship go beyond mere denial of information. They aim to normalize (or even legalize) Internet control, and include targeted viruses and the strategically timed deployment of distributed denial-of-service (DDoS) attacks, surveillance at key points of the Internet's infrastructure, take-down notices, stringent terms of usage policies, and national information shaping strategies [20]. Measures of control also include Internet curfews (i.e. the Internet is down for a few hours) and Internet blackouts (i.e. when there is no Internet access for up to several days). Internet censorship is sometimes used as a 'weapon' to suppress the dissemination of information and to stifle dissent; it can be done through harassment of those who publish information online (i.e. through fear) [21].

A comprehensive review of tools and technology for Internet filtering (including surveillance and non-technical censorship methods) is outlined by Murdoch and Anderson (2008). Filtering mechanisms include:

- **TCP/IP header filtering:** The censor's router can inspect the Internet Protocol [IP] address and port number of the destination. If the destination is found to be on a blacklist, the connection is dropped or redirected to a page indicating that access to the destination is denied.
- **TCP/IP content filtering:** The censor's router inspects the packet contents for any patterns or keywords that may be blacklisted. The focus is not on content, but on where packets are going to or coming from.
- **Domain Name Server (DNS) Tampering:** Normally, domain name servers are accessed by user computers to retrieve the corresponding IP address of a given domain. Through domain name server tampering, domain name resolution could fail as the router could send back an erroneous response that does not contain the right IP address; hence the connection fails.
- **Hyper Text Transfer Protocol (HTTP) Proxy Filtering:** In some cases users are forced to use HTTP proxies that are assigned for accessing the Internet. Those proxies may be the only way to reach the Internet and hence all traffic that goes through the proxies can be monitored. This is more powerful than TCP/IP headers and DNS filtering.
- **Hybrid TCP/IP and HTTP Proxy filtering:** Because using

HTTP Proxy Filtering is often demanding, a solution was devised to use only HTTP Proxy filtering for a list of IP addresses known to have prohibited content. If any of those IP addresses is accessed, traffic is redirected to a transparent HTTP proxy, which inspects the transferred stream and filters any banned content.

- **Denial-of-Service (DoS) attacks:** Denial-of-service attacks can be launched on a host server. A large number of computers request services from a particular server overwhelming it with too much traffic and causing the server and its connection to stall.
- **Server takedown:** Through legal, extra-legal or pressure methods, a company hosting a specific server could take it down and disconnect it from the Internet. The owner of the server may be able to transfer the server's contents however – provided that a backup copy exists – to another hosting company within hours.
- **Surveillance:** Constant technical monitoring through logging transfers between the host and the Internet user. If banned content is found in the transferred stream, actions – legal or extra-legal – could be taken against the user, the host or both. Such acts could trigger a sense of fear, causing the host to refrain from publishing such content and causing the user to hesitate from accessing it.
- **Social techniques:** This includes the requirement to show photo identification (ID) before using public computers at libraries or Internet cafés; social or religious norms that force Internet users to avoid opening particular content, and families placing the computer in the living room is another example of a social technique of censorship.

### 3. TOOLS AND TECHNIQUES TO BYPASS FILTRATION

A key component for any censorship resistant system or circumvention technology is to ensure *privacy* by enabling users to communicate undetected in a censorship network. This is often accomplished by incorporating certain techniques such as pseudonymity and anonymity into the system. However, previous research suggests that current techniques to ensure privacy still reveal a significant amount of identifying information [22]. In addition to addressing the limitations for ensuring privacy using tools other research has introduced four properties: anonymity, unlinkability, unobservability and pseudonymity, and a set of anonymity metrics, which can be used to improve the design and evaluation of censorship resistant systems [23].

So far the analysis of previous research has identified two main challenges for designing censorship resistant systems. These challenges include research focused on content protection and anonymity to ensure privacy. In addition to content protection and anonymity other approaches for designing censorship resistant systems have centered on issues related to *content filtering*. Therefore the main technical approaches for addressing challenges with designing censorship resistant systems include:

1. Anonymity,
2. Content protection, and
3. Content filtering.

In addition to the technical approaches and research on censorship resistant systems discussed above, several *social and behavioral methods* have also been investigated. For example, the first economic model of censorship resistance based on conflict theory and node preferences in a peer-to-peer system was presented by Danezis and Anderson (2004)[24].

Many different approaches to design censorship resistant systems have been proposed. The approaches so far have consisted of possible solutions from both technical and social perspectives. A comprehensive and successful Internet censorship strategy involves collaboration and coordination among various social, political and technological entities. Therefore, a solution to Internet censorship must attempt to exploit the vulnerabilities within each entity. A solution to Internet censorship may evolve from a technological perspective provided it is designed with the optimal combination of features including an underlying or indirect motive to destabilize social and political structures.

Several anti-censorship techniques have been developed to circumvent the aforementioned technical filtering methods. While there are many academic projects actively engaged in the development of circumvention technologies. The variety of commercial anti-censorship applications is based on one of the following circumvention methods described in **Table 1**[25].

Method	Definition
HTTP Proxy	HTTP proxying sends HTTP requests through an intermediate proxying server. A client connecting through an HTTP proxy sends exactly the same HTTP request to the proxy as it would send to the destination server unproxied. The HTTP proxy parses the HTTP request; sends its own HTTP request to the ultimate destination server; and then returns the response back to the proxy client.
CGI Proxy	CGI proxying uses a script running on a web server to perform the proxying function. A CGI proxy client sends the requested URL embedded within the data portion of an HTTP request to the CGI proxy server. The CGI proxy server pulls the ultimate destination information from the data embedded in the HTTP request, sends out its own HTTP request to the ultimate destination, and then returns the result to the proxy client.
IP Tunneling	Some of the most common tools used for IP Tunneling include virtual private networks or VPNs. VPNs give the user client a connection that originates from the VPN host rather than from the location of the client. Thus a client connecting to a VPN in a non-filtered country from a filtered country has access as if he is located in the non-filtered country.
Re-routing	Re-routing systems route data through a series of proxying servers, encrypting the data again at each proxy, so that a given proxy knows at most either where the traffic came from or where it is going to, but not both.

Distributed Hosting	A distributed hosting system mirrors content across a range of participating servers that serve the content out to clients upon request. The primary advantage of a distributed hosting system is that it provides access to the requested data even when the original server cannot, for instance if the original server has been overwhelmed by traffic or even taken down by a denial of service attack
---------------------	--

Table 1

### 3.1 Proxy Software

Proxy software allows you to retrieve a Web site or other Internet resource even when direct access to that resource is blocked from your location. There are many different kinds of proxies, including:

- Web proxies, which only require that you know the proxy Web site's address. A Web proxy URL may look like <http://www.example.com/cgi-bin/nph-proxy.cgi>.
- HTTP proxies, which require that you or a piece of software modify your browser settings. HTTP proxies only work for Web content. You may get the information about a HTTP proxy in the format "proxy.example.com:3128" or "192.168.0.1:8080".
- SOCKS proxies, which also require that you or a piece of software modify your browser settings. SOCKS proxies work for many different Internet applications, including e-mail and instant messaging tools. The SOCKS proxy information looks just like HTTP proxy information.

Once you are viewing a page through a Web proxy, you should be able to use your browser's forward and back buttons, click on links and submit forms without losing your proxied connection to the filtered site. This is because your proxy has rewritten all of the links on that page so that they now tell your browser to request the destination resources through the proxy.

You can find Web proxy URLs at sites such as <http://www.proxy.org>, by signing up for a mailing list such as the one at <http://www.peacefire.org/circumventor>, by following a country-specific twitter feed, or simply by searching for "free Web proxy" in a search engine. Proxy.org lists thousands of free Web proxies. The 10 web proxies we will analyze are

1. Free gate
2. Ultra Surf
3. G Tunnel
4. Tor
5. GappProxy
6. Hyk-proxy
7. Your Freedom
8. GPass
9. Tunnelier
10. Psiphon

### 3.2 VPN or Virtual Private Network Service

A VPN (virtual private network) is a network that can use the internet to provide secure connections between one or more devices for data exchange. A VPN can open a secure interconnection or "tunnel" between different devices and the data that passes through the tunnel can be encrypted as a method

of security so that the data passing through the tunnel cannot be read. A virtual private network encrypts and tunnels all Internet traffic between yourself and another computer. This computer might belong to a commercial VPN service, your organization, or a trusted contact.

Because VPN services tunnel all Internet traffic, they can be used for e-mail, instant messaging, Voice over IP (VoIP) and any other Internet service in addition to Web browsing, making everything that travels through the tunnel unreadable to anyone along the way. If the tunnel ends outside the area where the Internet is being restricted, this can be an effective method of circumvention, since the filtering entity/server sees only encrypted data, and has no way of knowing what data is passing through the tunnel. It has the additional effect of making all your different kinds of traffic look similar to an eavesdropper.

Since many international companies use VPN technology to allow employees who need access to sensitive financial or other information to access the companies' computer systems from home or other remote locations over the Internet, VPN technology is less likely to be blocked than the technologies used only for circumvention purposes. It is important to note that the data is only encrypted as far as the end of the tunnel, and then travels unencrypted to its final destination.

There are a number of different standards for setting up VPN networks, including IPSec, SSL/TLS and PPTP that vary in terms of complexity, the level of security they provide, and which operating systems they are available for. Naturally, there are also many different implementations of each standard within software that have various other features.

- While PPTP is known to use weaker encryption than either IPSec or SSL/TLS, it may still be useful for bypassing Internet blocking, and the client software is conveniently built into most versions of Microsoft Windows.
- SSL/TLS-based VPN systems are relatively simple to configure, and provide a solid level of security.
- IPSec runs at the Internet level, responsible for packet transfer in the Internet architecture, while the others run at the Application level. This makes IP sec more flexible, as it can be used for protecting all the higher level protocols, but also difficult to set up.

The 10 virtual private network services we will analyze are

1. ProXPN
2. SecurityKiss
3. Hotspot Shield
4. UltraVPN
5. FreeVPN
6. CyberGhost
7. AirVPN
8. VPNod
9. ItsHidden
10. OpenVPN

### 4. CONCLUSION: PROXY OR VPN

The purpose of using both VPN and proxy servers is to conceal the users identity, or to spoof a certain geo-location. Although

performing a similar function, the actual processes involved are very different, and therefore have very different consequences.

#### 4.1 Proxy Software

##### 4.1.1 Compatibility Issues with Web Proxies

Web proxies only work for Web traffic, so they cannot be used for other Internet services such as e-mail or instant messaging. Many are also incompatible with complex Web sites like Facebook, streaming multimedia content on sites such as YouTube, and encrypted sites that are accessed through HTTPS. Worse yet, some Web proxies cannot themselves be accessed through HTTPS. If you use such a proxy to log in to a destination site that is normally secure, you may be putting your sensitive information, including your password, at risk.

##### 4.1.2 Security Risks with Web Proxies

You should be aware of some of the risks associated with the use of Web proxies, particularly those operated by individuals or organizations you do not know. If you use a Web proxy simply to read a public Web site such as [www.bbc.co.uk](http://www.bbc.co.uk), your only real concerns are that:

- Someone might learn that you are viewing a censored news source.
- Someone might learn which proxy you rely on to do so.

##### 4.1.3 Obfuscation is not Encryption

Some Web proxies, most notably those that lack support for HTTPS, use simple encoding schemes to circumvent poorly-configured domain name and keyword filters. Proxy designers have found this trick useful even in countries where keyword filtering is not present, because Web proxies often include the target URL inside the actual URL that your browser sends to the proxy every time you click on a link or submit a new address.

##### 4.1.4 Anonymity Risks with Web Proxies

Tools designed to circumvent filtering do not necessarily provide anonymity, even those that might include words like “anonymizer” in their names! In general, anonymity is a much more elusive security property than basic confidentiality (preventing eavesdroppers from viewing the information that you exchange with a Web site) and, as discussed above, even to ensure basic confidentiality through a Web proxy requires, at the very least, that you:

- use an HTTPS Web proxy
- connect through that proxy to an HTTPS destination Web site
- trust the proxy administrator’s intentions, policies, software and technical competence

##### 4.1.5 Advertising, Viruses and Malware

Some of the people who set up Web proxies do it to make money. They may do this simply and openly by selling advertisements on each proxied page.

##### 4.1.6 Cookies and Scripts

There are also risks associated with the use of cookies and embedded scripts. Many Web proxies can be configured to remove cookies and scripts, but many sites (for example, social networking sites like Facebook and media streaming sites

like YouTube) require them to work properly. Web sites and advertisers can use these mechanisms to track you, even when you use proxies, and to produce evidence that, for example, the person who did one thing openly is the same person who did another thing anonymously.

#### 4.2 VPN or Virtual Private Network

##### 4.2.1 Security Issues

One of the advantages of using a VPN is that it allows remote users to securely access the enterprise’s systems. Unfortunately, this also makes the network susceptible to security breaches. Often, a remote user will use unsecured assets, such as a personal laptop, to access the enterprise’s network. If this device has a virus or some other malicious software, it can compromise the network once the user has authenticated his access request and successfully logged on to the servers.

##### 4.2.2 Performance Issues

Leased lines or a dedicated data services can give an organization guaranteed bandwidth regardless of the traffic load on the network or the requirements of competing entities. In contrast, there can be no bandwidth guarantee on public networks unless elaborate resource sharing protocols such as MPLS are used.

Similarly, it might be difficult to get VPN solutions from different providers to work with each other due to the different standards and protocols that may be in use. This should become less of an issue as service providers adopt more generally accepted standards and the industry becomes more mature.

##### 4.2.3 Complexity

VPNs often use multiple network topologies, protocols, network hardware equipment and service providers to establish a single VPN tunnel. Using several data services providers can make a network more robust, but at the same time, trying to get several network components to work well together can only create complexity, especially if most of these components weren’t designed to work together.

#### 4.3 Summary

VPN is superior in almost every way to proxies. It provides vastly improved online anonymity, and protects your entire on-line life.

Base	Proxy	VPN
Online Security	It gives very low-level security. Only on SSL connection everything is encrypted but on non-SSL connection everything is vulnerable to cyber threats.	It gives high-level encryption up to 256-bit. VPN is more like a safe vault, once you have availed it, all your communications are completely secure.
Online Privacy	When using a Proxy, anyone can intercept your private data.	With VPN all your data is totally encrypted and therefore no one can intrude in your privacy, not even your ISP can monitor your activities.

Online Freedom	It only works for certain geo-restrictions and cannot help you bypass strong firewalls and censorship.	With VPN, you can access any website from anywhere in the world.
Speed	It does compromise your internet speed to great extent due to overloaded servers.	With VPN, you can avail best solutions to boost up your internet speed such as SmartDNS. VPN doesn't compromise your internet speed.
Compatibility	It is limited only to certain browsers.	It works with all OS and devices such as Windows, Android, iOS, Linux, Mac and Routers.
Reliability	Only works for bypassing geo-restricted channels and provides no security at all. Hence, not reliable.	It is the most sophisticated tool to ensure your online security, privacy and freedom at same time. Hence, 100% reliable.
Stability	It usually crashes most of the time. It gives maximum downtime, even when you are in the middle of downloading or streaming.	VPN is 99.9% stable and provides you maximum up-time.

Table 2

## REFERENCES

- Ben Segal (1995). "A Short History of Internet Protocols at CERN".
- Réseaux IP Européens (RIPE)
- "Internet History in Asia". 16th APAN Meetings/Advanced Network Conference in Busan.
- Cohen, T. 1997. Censorship and the regulation of speech on the internet. Johannesburg : Centre for Applied Legal Studies.
- Akdeniz, Y. and Altıparmak, K. 2008. Internet: restricted access: a critical assessment of internet content regulation and censorship in Turkey. [http://privacy.cyber-rights.org.tr/?page\\_id=256](http://privacy.cyber-rights.org.tr/?page_id=256).
- Deibert, R. and Rohozinski, R. 2010. Liberation vs control: the future of cyberspace, *Journal of democracy* 24(1): 43-57.
- Akdeniz, Y. 2007. Governing racist content on the internet: national and international responses. *University of New Brunswick law journal* 56: 103-161.
- Peace, A. 2003. Balancing free speech and censorship: academia's response to the internet. *Communications of the Association for Computing Machinery* 46(11): 105-109.
- Clyde, A. 1997. Censorship or protection? Children and access to the internet. *Emergency librarian* 24(3): 48-50.
- Bailey, M. and Labovitz, C. 2011. Censorship and co-option of the internet infrastructure. Technical report, CSE-TR-572-11. <http://nsrg.eecs.umich.edu/publications/CSE-TR-572-11.pdf>.
- Malley, I. 1990. Censorship and libraries .London: Library Association Publishing.
- "ONI Country Profile: India" (<http://access.opennet.net/wpcontent/uploads/2011/12/accesscontestedindia.pdf>), Access Contested, Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain(Eds), OpenNet Initiative, MIT Press, November 2011, pp. 299308
- "Internet Freedom" (<http://www.state.gov/g/drl/rls/hrrpt/2010/sca/154480.htm>), 2010 Country Reports on Human Rights Practices: India, Bureau of Democracy, Human Rights, and Labor, U.S. Department of State, 8 April 2011
- "Indian Computer Emergency Response Team" (<http://www.certin.org.in/>), website, Department of Information Technology, Ministry of Communications and Information Technology, Government of India
- CERTIN "Charter and Mission" (<http://www.certin.org.in/s2cMainServlet?pageid=CHARTMISSION>), Indian Computer Emergency Response Team, Department of Information Technology, Ministry of Communications and Information Technology, Government of India
- Due to legal concerns the OpenNet Initiative does not check for filtering of child pornography and because their classifications focus on technical filtering, they do not include other types of censorship.
- Internet Enemies ([http://march12.rsf.org/i/Report\\_EnemiesoftheInternet\\_2012.pdf](http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf)), Reporters Without Borders (Paris), 12 March 2012
- <https://freedomhouse.org/report/freedomnet/2011/india>
- "India Country Report" (<http://www.freedomhouse.org/sites/default/files/India%202012.pdf>), Freedom on the Net 2012, Freedom House.
- Deibert, J.G., Palfrey, R., Rohozinski, R. and Zittrain, J. eds. 2010. Access controlled: the shaping of power, rights, and rule in cyberspace. Cambridge, MA: MIT Press.
- Grothoff, et al. C. 2003. An encoding for censorship-resistant sharing. Technical report. <http://www.cs.helsinki.fi/u/jtindgr/stuff/ecrs.ps>.
- J. R. Rao and P. Rohatgi. Can pseudonymity really guarantee privacy? In Proceedings of the Ninth USENIX Security Symposium, pages 85–96. USENIX, Aug. 2000. <[http://www.usenix.org/publications/library/proceedings/sec2000/full\\_papers/rao/rao.pdf](http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/rao/rao.pdf)>.
- George Danezis and Claudia Diaz. A survey of anonymous communication channels. Technical Report MSRTR-2008-35, Microsoft Research, January 2008.
- George Danezis and Ross Anderson. The economics of censorship resistance. In The Third Annual Workshop on Economics and Information Security (WEIS04), 2004.
- Roberts et al, "2007 Circumvention Landscape Report: Methods, Uses, and Tools," The Berkman Center for Internet & Society at Harvard University, March 2009